ANEXO: SEGURIDAD DE LA INFORMACIÓN, PRIVACIDAD DE LA INFORMACIÓN Y PROPIEDAD INTELECTUAL

CAPÍTULO I - SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO

1.1 SEGURIDAD DE LA INFORMACIÓN

EL CONTRATISTA y/o **CONTRAPARTE,** manifiesta que conoce y acepta las políticas corporativas de Seguridad de la información y Ciberseguridad y tratamiento de datos personales, las cuales se encuentran disponibles en los siguientes vínculos: https://www.colsubsidio.com/hubfs/documentos/colsubsidio/politicas-de-seguridad-de-la-informacion-gerencia-corporativa-de-tecnologia.pdf y Manual interno de políticas y procedimientos para el tratamiento de datos personales obligándose al cumplimiento de estas en la ejecución de la relación negocial y, en especial, a cumplir con los procedimientos y estándares de **COLSUBSIDIO** que se le proporcionen. Así mismo se obliga a consultar periódicamente las Políticas Corporativas mencionadas. **COLSUBSIDIO** se reserva el derecho de actualizarlas.

1.1.1. Las siguientes son obligaciones especiales del **EL CONTRATISTA** y/o **CONTRAPARTE** relacionadas con Seguridad de la información:

1.1.1.1. **EL CONTRATISTA** y/o **CONTRAPARTE** deberá asegurar que todo el personal que tenga acceso a la información de **COLSUBSIDIO** cuente con acuerdo de confidencialidad y esté obligado a no revelar, divulgar, exhibir, mostrar, comunicar, utilizar y/o emplear la Información de **COLSUBSIDIO** en beneficio propio o de un tercero.

1.1.1.2. **EL CONTRATISTA** y/o **CONTRAPARTE** deberá alinear sus procesos de seguridad de la Información con estándares reconocidos por la industria para la confidencialidad, integridad y disponibilidad de la Información**.**

1.1.1.3. **EL CONTRATISTA y/o CONTRAPARTE** deberá contar con procedimientos de manejo seguro para documentos físicos y/o medios electrónicos que contenga datos e información confidencial y/o sensible de **COLSUBSIDIO,** incluidas prácticas seguras de transporte, transferencia, tratamiento, manejo, almacenamiento y procedimientos de eliminación segura, para garantizar que la información confidencial y/o sensible no pueda recuperarse ni reconstruirse, luego de ser eliminada.

1.1.1.4. **EL CONTRATISTA** y/o **CONTRAPARTE** deberá devolver a **COLSUBSIDIO,** los documentos físicos y/o medios electrónicos que contenga datos e información confidencial y/o sensible de **COLSUBSIDIO,** a más tardar dentro de los diez (10) días hábiles siguientes a la fecha de terminación de la relación negocial con **COLSUBSIDIO**, a menos que **COLSUBSIDIO** le diera instrucciones por escrito para que proceda a su destrucción, entregando a **COLSUBSIDIO** la constancia a través de documento suscrito por su Representante Legal de la destrucción o eliminación controlada de la información.

1.1.1.5. **COLSUBSIDIO** se reserva el derecho de realizar auditorías, evaluaciones e inspecciones de seguridad de los sistemas, procesos e instalaciones del CONTRATISTA y/o **CONTRAPARTE,** subcontratistas y/o terceros involucrados en el manejo de información confidencial y/o sensible de **COLSUBSIDIO;** a su turno, **CONTRATISTA** y/o **CONTRAPARTE,** se obliga a permitir estas auditorias, evaluaciones y/o inspecciones,

Vigilado Supersubsidio

incluso frente a sus subcontratistas. para garantizar el cumplimiento de los requisitos de seguridad de este Anexo.

1.1.1.6. **EL CONTRATISTA** y/o **CONTRAPARTE** cooperará plenamente con **COLSUBSIDIO** y proporcionará toda la información necesaria, acceso y asistencia para facilitar dichas auditorías, evaluaciones e inspecciones. **EL CONTRATISTA** y/o **CONTRAPARTE** remediará cualquier deficiencia de seguridad o incumplimiento identificado dentro de un plazo razonable acordado con **COLSUBSIDIO.**

1.1.1.7. **EL CONTRATISTA** y/o **CONTRAPARTE** deberá asegurar que todo el personal, que tenga acceso a la información de **COLSUBSIDIO** reciba capacitación y concientización en materia de seguridad de la información la cual incluya temas como: protección de datos, manejo o tratamiento de información, confidencialidad y procedimientos de la gestión de incidentes de seguridad de la información y responsabilidad sobre el manejo de la información.

1.1.1.8. **EL CONTRATISTA** y/o **CONTRAPARTE** realizará verificaciones de antecedentes penales y de riesgos, de todo el personal que tenga acceso a la información de COLSUBSIDIO, de acuerdo con las leyes y regulaciones aplicables, tomando acciones de corrección o mitigación de riesgos según los hallazgos de las verificaciones.

1.1.1.9. **El CONTRATISTA** y/o **CONTRAPARTE** mantendrá registros detallados de las actividades de capacitación y concientización realizadas incluidos registros de asistencia, materiales de capacitación y evaluaciones, y pondrá dichos registros a disposición de COLSUBSIDIO cuando lo solicite para fines de auditoría, evaluaciones e inspecciones.

1.1.1.10. Durante la vigencia de la relación negocial y por un periodo de cinco (5) años adicionales contados a partir de su finalización**, EL CONTRATISTA** y/o **CONTRAPARTE** y el personal que éste vincule para el desarrollo de actividades, deberán guardar absoluta confidencialidad acerca de la información que por razones de la ejecución de la relación negocial llegaren a conocer de COLSUBSIDIO, lo que incluye pero no se limita a operaciones, procesos internos, así como información comercial, profesional, técnica y/o financiera, de tal manera que únicamente se utilice con la finalidad de dar pleno cumplimiento al objeto de la relación negocial.

Tendrá el carácter de confidencial toda información comercial, estratégica, profesional, técnica, financiera, jurídica y de cualquier tipo a que tenga acceso EL **CONTRATISTA** y/o **CONTRAPARTE** con ocasión o en desarrollo de las actividades incluidas en el objeto de la relación negocial, cualquiera que sea la forma y formato en que pueda llegar a conocerla.

1.1.2. Las relaciones negociales que impliquen la entrega de bases de datos, que contengan datos o información confidencial y/o sensible y sean suministradas por **COLSUBSIDIO,** deberán contar con Contrato de confidencialidad. **COLSUBSIDIO** realizará la transferencia de información confidencial y/o sensible a través de los canales autorizados por la Gerencia de Riesgos y Cumplimiento.

Vigilado Supersubsidio

1.2. CIBERSEGURIDAD

1.2.1. Las siguientes son obligaciones especiales del **EL CONTRATISTA** y/o **CONTRAPARTE** relacionadas con Ciberseguridad:

1.2.1.1. **El CONTRATISTA** deberá contar con un plan de respuesta a incidentes para detectar, responder y mitigar los incidentes de seguridad y las violaciones a la información, el cual deberá ser activado ante cualquier incidente y vulnerabilidades de seguridad, violación o acceso no autorizado a los datos o sistemas de información propios que pudieren llegar o afecten a COLSUBSIDIO a los correos electrónicos cggersfp@colsubsidio.com dentro de las 24 horas al incidente y proporcionar a **COLSUBSIDIO** actualizaciones periódicas sobre la investigación y la remediación.

1.2.1.2. **EL CONTRATISTA** y/o **CONTRAPARTE** cooperará plenamente con **COLSUBSIDIO** en la investigación y resolución de cualquier incidente de seguridad o violación de datos y tomará las medidas necesarias para mitigar el daño potencial y prevenir sucesos futuros.

1.2.1.3. **EL CONTRATISTA** y/o **CONTRAPARTE** deberá realizar una revisión preventiva y general de los sistemas de información, que incluya un proceso de identificación y mitigación de vulnerabilidades encontradas e informar el resultado de la revisión a **COLSUBSIDIO** dentro de las 24 horas siguientes a la revisión del sistema.

1.2.1.4. **EL CONTRATISTA** y/o **CONTRAPARTE** implementará un programa de gestión de vulnerabilidades que incluya escaneo regular de vulnerabilidades con terceros, evaluación de riesgos y parcheo de vulnerabilidades identificadas en el software, los sistemas y la infraestructura que soporta la información de **COLSUBSIDIO**.

1.2.1.5. Si **EL CONTRATISTA** y/o **CONTRAPARTE** cuenta con servicios en la nube y se encuentra ahí la información de **COLSUBSIDIO, EL CONTRATISTA** y/o **CONTRAPARTE** deberá garantizar que existan controles de seguridad, incluyendo la separación lógica de los datos, la seguridad de múltiples inquilinos, los controles de acceso basados en roles y el cumplimiento de las mejores prácticas y estándares de seguridad en la nube.

1.2.1.6. **Obligaciones adicionales para proveedores de servicios tecnológicos**

1.2.1.6.1. SI **El CONTRATISTA** y/o **CONTRAPARTE** es un proveedor de servicios tecnológicos o si el objeto negocial supone la prestación de servicios tecnológicos**, El CONTRATISTA** y/o **CONTRAPARTE** deberá contar con prácticas seguras de diseño y desarrollo de software, codificación segura, revisión de código, análisis de código estático y dinámico, pruebas de seguridad durante todo el ciclo de vida de desarrollo de software (SDLC).

1.2.1.6.2. **El CONTRATISTA y/o CONTRAPARTE** remediará cualquier deficiencia identificada, dentro de un plazo razonable acordado con COLSUBSIDIO, adicionalmente proporcionará la arquitectura detallando los controles de seguridad, mecanismos de cifrado y diagramas de flujo de datos.

1.2.1.6.3. **El CONTRATISTA** y/o **CONTRAPARTE** remediará cualquier deficiencia identificada, dentro de un plazo razonable acordado con COLSUBSIDIO, adicionalmente proporcionará la arquitectura detallando los controles de seguridad, mecanismos de cifrado y diagramas de flujo de datos.

Vigilado Supersubsidio

1.2.1.6.4. **El CONTRATISTA** y/o **CONTRAPARTE** deberá contar con cifrados actualizados para transmitir y almacenar los datos y la información de **COLSUBSIDIO**, manteniendo así los protocolos seguros de transferencia de archivos (SFTP).

1.3 CONTINUIDAD DE NEGOCIO

1.3.1 Las siguientes son obligaciones especiales de **EL CONTRATISTA** y/o **CONTRAPARTE** relacionadas con Continuidad del Negocio:

1.3.1.1 **EL CONTRATISTA** y/o **CONTRAPARTE** deberá contar con un plan de continuidad del negocio que garantice la continuidad en la entrega de los productos y/o servicios para **COLSUBSIDIO**, el cual debe incluir estrategias de mitigación de riesgos, procesos de recuperación con tiempos máximos tolerables (MTPD), y tiempos objetivos de recuperación (RTO).

1.3.1.2 **EL CONTRATISTA** y/o **CONTRAPARTE** deberá notificar a **COLSUBSIDIO** los canales de comunicación y procedimientos de notificación en caso de indisponibilidad de los sistemas tecnológicos e incidentes de seguridad de la información, que afecten la prestación de los servicios para **COLSUBSIDIO**, incluyendo puntos de contacto designados.

CAPÍTULO II - PRIVACIDAD DE LA INFORMACIÓN.

2.1 **EL CONTRATISTA** y/o **CONTRAPARTE** cuando en la ejecución del objeto negocial ejecute la recolección, uso y/o manejo de los datos personales de los clientes y/o personas naturales relacionadas con **COLSUBSIDIO,** asume la calidad de encargado del tratamiento de la base de datos y **COLSUBSIDIO** la calidad de responsable del tratamiento, de acuerdo con la Ley 1581 de 2012 y sus decretos reglamentarios. Por lo tanto, **EL CONTRATISTA** y/o **CONTRAPARTE** deberá tratar los datos exclusivamente con la finalidad autorizada por el titular del dato y lo dispuesto por **COLSUBSIDIO**. Las relaciones negociales que impliquen la entrega de bases de datos, que contengan datos personales y sean suministradas por **COLSUBSIDIO,** deberán contar con Contrato de Tratamiento de Datos Personales.

2.2 En todo caso **EL CONTRATISTA** y/o **CONTRAPARTE** deberá cumplir la Política de Tratamiento de Datos Personales del **COLSUBSIDIO**, que declara conocer y aceptar, disponible en www.colsubsidio.com, así como contar con una Política propia, que en todo caso debe cumplir la normativa y regulación de Datos Personales. De otra parte, cuando la ejecución de la relación negocial suponga el uso de bases de datos de **EL CONTRATISTA** y/o **CONTRAPARTE** como responsable, **COLSUBSIDIO** asumirá la calidad de encargado del tratamiento. De igual manera **EL CONTRATISTA** y/o **CONTRAPARTE** indemnizará los perjuicios que pueda llegar a causar a COLSUBSIDIO como resultado del incumplimiento de los principios aplicables al tratamiento de la información personal, así como de las sanciones que llegare a imponerse. Lo anterior sin perjuicio que **COLSUBSIDIO**

Vigilado Supersubsidio

pueda llamar al **CONTRATISTA** y/o **CONTRAPARTE** en garantía dentro de un eventual proceso judicial o administrativo que se llegare a adelantar por la ocurrencia de dichas circunstancias. Adicionalmente, en caso de presentarse una queja o reclamación ante cualquier autoridad judicial o administrativa en relación con el Tratamiento de los datos personales, **EL CONTRATISTA** y/o **CONTRAPARTE** asumirá de inmediato la defensa de **COLSUBSIDIO** totalmente a su costo.

CAPÍTULO III - PROPIEDAD INTELECTUAL

3.1 En todo negocio jurídico en el que participe **COLSUBSIDIO**, **EL CONTRATISTA** y/o **CONTRAPARTE** deberá asegurar la utilización correcta de propiedad intelectual de terceros que sea utilizada en la ejecución del objeto negocial, y/o suministro del servicio y/o bien, asegurando contar con la debida autorización cuando aplique y manteniendo indemne a **COLSUBSIDIO** de cualquier infracción de derechos.

3.2 En los negocios jurídicos en el que participe **COLSUBSIDIO** tales como consultorías, prestación de servicios, diseño, desarrollos, alianzas o convenios, entre otros se deberá identificar los activos intangibles que puedan generarse a favor de **COLSUBSIDIO,** bajo las siguientes premisas**:**

3.2.1 **El CONTRATISTA** debe garantizar la correcta cesión de derechos patrimoniales de dichos activos intangibles a favor de **COLSUBSIDIO** por haber sido obras por encargo bajo el principio contenido en los Artículos 28 y 29 de la ley 1450 de 2011 o demás normas que lo modifiquen o complementen**.** Como un entregable de todos los proyectos desarrollados se deberá incluir la documentación requerida para hacer el respectivo registro de propiedad intelectual ante la entidad correspondiente.

3.2.2 Para los negocios jurídicos en los que se identifique la creación de propiedad intelectual, el área de **COLSUBSIDIO** responsable de la ejecución, acorde con la política de propiedad intelectual interna de **COLSBUSIDIO** deberá acordar con la **CONTRAPARTE** el tratamiento que se le dará a la propiedad intelectual que el negocio jurídico pueda generar.

CAPÍTULO IV – CONTRATISTAS Y SUBCONTRATISTAS

Si **EL CONTRATISTA** y/o **CONTRAPARTE** contrata o subcontrata a proveedores de serviciosg6 externos para cumplir sus obligaciones frente a **COLSUBSIDIO, EL CONTRATISTA** y/o **CONTRAPARTE** deberá garantizar que dichos terceros cumplan con los anteriores requisitos y obligaciones a él solicitados en este anexo.

EL CONTRATISTA y/o **CONTRAPARTE** seguirá siendo plenamente responsable de los actos y omisiones de sus subcontratistas o proveedores de servicios externos que utilice para el cumplimiento de sus obligaciones y/o compromisos frente a **COLSUBSIDIO**

Versión 1
Aprobó: Gerente de Riesgos y Cumplimiento

Vigilado Supersubsidio